Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Leonardo Miranda do Nascimento

REDES SENSORES SEM FIO: Aplicada em Ambientes Militares

Rio de Janeiro

2016

Leonardo Miranda do Nascimento

REDES SENSORES SEM FIO: Aplicada em Ambientes Militares

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro ï NCE/UFRJ.

Orientador:

Claudio Miceli de Farias, D.Sc., UFRJ, Brasil

Rio de Janeiro

2016

Leonardo Miranda do Nascimento

REDES SENSORES SEM FIO:

Aplicada em Ambientes Militares

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2016.

Claudio Miceli de Farias, D.Sc., UFRJ, Brasil

RESUMO

NASCIMENTO, Leonardo Miranda do. **REDES SENSORES SEM FIO: Aplicada em Ambientes Militares**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2016.

Nos últimos tempos o avanço tecnológico, em diversas áreas, foi enorme, em especial nas áreas de sensores. A possibilidade de efetuar monitoramento, controle e realizar a tomada de determinadas decisões com a computação não presencial, além de facilitar a vida das pessoas, possibilitou a exploração de outras áreas, em que antes, a interação humana era fundamental. O objetivo deste trabalho é mostrar a atuação das redes sensores no setor Militar, explorando as possibilidades e mostrando pontos positivos e negativos. Primeiramente, uma abordagem geral das Redes Sensores Sem Fio (RSSF) será apresentada. Em seguida, a segurança necessária para a aplicação de redes sensores em um ambiente, onde o sigilo é fundamental, também será abordada. Vulnerabilidades e ataques serão descritos e, finalmente, os protocolos de segurança e otimização de energia bem como os tipos de roteamentos serão apresentados.

ABSTRACT

NASCIMENTO, Leonardo Miranda do. **REDES SENSORES SEM FIO: Aplicada em Ambientes Militares**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2016.

Lately technological advances in several areas was huge, especially in sensors areas. The ability to perform monitoring, control and make the taking of certain decisions, with no face computing, besides facilitating the lives of people allowed to exploring other areas where before human interaction was essential. The objective of this study is to show the performance of the sensor networks in military sector exploring the possibilities and showing positive and negative points. First an overview of the Wireless Sensor Networks (WSN) will be displayed. Then the security necessary for the application of sensor networks in an environment where confidentiality is key, will also be demonstrate. Vulnerabilities and attacks will be described and, finally, energy security and optimization of protocols and types of routes are displayed.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

API ï Application Programming Interface
DS ï Sistema de Distribuição
DSM ï Distribuição de Sistema Médium
DSSS ï Direct Sequence Spread Spectrum
ERB ï Estação Rádio Base
FHSS ï Frequency Hopping Spread Spectrum
IEEE ï Institute of Eletrical and Eletronics Engineers
INSENS ï Intrusion-Tolerant Routing Protocol for Wireless Sensor Networks
LAN ï Local Area Network
MAC ï Código de Autenticação de Mensagem
MEMS ï Micro Sistemas Eletro Mecânicos
MANET ï Mobile Ad hoc NETwork
NCAP ï Networking Capable Applications Processor
PHY ï Phisico
RSSF ï Redes Sensores Sem Fio
SPINS ï Security Protocols for Sensor Networks
S-MAC ï Sensor Medium Access Control
TCP ï Transmission Control Protocol
TIM ï Transducer Interface Module
TEDS ï Transducer Electronic Data Sheets (TEDS)
VANT ï Veículo Aéreo não Tripulado
WM ï Wireless Médium
WTIM ï Wireless Transducer Interface Module

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica introduziu na sociedade atual muitos benefícios e facilidades. Neste sentido micro sistemas eletro mecânicos (MEMS ï *Micro Electro Mecanical System*) e comunicação sem fio tem sido o estopim para o desenvolvimento de redes sensores. Existe uma forte tendência para a chamada ñcomputação não presencialò (DUTRA, 2012), este tipo de computação será alicerçado em sensores que irão interagir entre si, trocando informações e auxiliando na tomada de decisão pela alta administração, para isso, é primordial que a popularização desta tecnologia ocorra no que diz respeito a custo, propiciando um maior investimento tecnológico e consequentemente novas melhorias, os desafios de software, hardware e sociais também são grandes.

Redes Sensores Sem fios RSSF são formadas por um grande número de ***ñnósò*** sensores, que devem ser capazes de monitorar algum tipo de evento físico e reportar a um observador. Neste contexto existem as MANET *(Mobile Ad hoc NETwork),* no que diz respeito a questões organizacionais RSSF e MANET são idênticas, haja vista que a comunicação entre os ***ñnósò*** é feita por meio de uma rede *Ad-Hoc* wireless, um ñóò passando para outro os dados obtidos no sensoriamento e assim por diante (DUTRA, 2012).

A diferença está no fato das MANET viabilizar a comunicação entre os ñósò sensores, que podem estar executando funções distintas, enquanto uma RSSF tende a exercer uma função mais colaborativa, em que os ñósò passam os dados para um observador. Neste contexto, o protocolo de roteamento deve se adaptar a

essas novas características, que não estão presentes em redes estruturadas comuns, como por exemplo, a limitação de recursos bem como a topologia dinâmica (DUTRA, 2012).

Devido à popularização e aplicação diversa, com um alto grau de acurácia, nos dados fornecidos, e uma tecnologia em crescente evolução, a quantidade de dados fornecidos por uma RSSF é consideravelmente elevada nos dias de hoje, se comparada a outras épocas do passado. O grande desafio é exatamente filtrar estas informações, que muitas vezes podem ser redundantes. Neste cenário, é de suma importância que haja um método para reunir e compilar os dados provenientes dos diversos sensores de uma RSSF, para que o operador possa ter subsídios na tomada de uma decisão mais adequada. Um problema presente, e que deve ser tratado, no monitoramento feito por RSSF, é a quantidade de dados apresentados pelas RSSF. Neste contexto, a Fusão de Dados figura como uma solução possível para o problema descrito, tratando uma gama de diferentes informações, oriundas de diversos dispositivos, sem negligenciar as questões de segurança.

1.1 OBJETIVO

A aplicação de redes sensores tem sido uma tendência cada vez mais atual em diversos seguimentos da sociedade como, por exemplo: controle, tráfego, ambiente e medicina. Abordaremos os desafios e os benefícios da aplicação de redes sensores no ambiente Militar.

1.2 ORGANIZAÇÃO DO TRABALHO

Este trabalho tem início com uma breve introdução, serão apresentados outros quatro capítulos que se propõem a discutir o tema em tela. O segundo capítulo faz

uma abordagem geral da RSSF e suas principais características, no intuito de apresentar embasamento aos próximos assuntos abordados em outros capítulos. O terceiro capítulo tem como objetivo fazer uma breve apresentação da família IEEE 1451, que tem o propósito de minimizar o problema decorrente do surgimento de inúmeros protocolos e especificações para as redes de controle, propondo interfaces padronizadas entre os transdutores e as redes, permitindo separar o projeto do transdutor da escolha da rede de controle, e abordar de forma sucinta a Fusão de Dados que auxilia no tratamento das diversas informações oriundas de diversos dispositivos. O quarto capítulo discute as possibilidades da aplicação de RSSF em ambientes e atividades Militares como vigilância do território Nacional, treinamento em campos de batalha, monitoramento por sonar e radar, e trata da segurança necessária para tal aplicação ser eficaz em ambientes onde possa garantir a confidencialidade dos dados, em que é primordial. O quinto capítulo apresenta um resumo de tudo que foi discutido ao longo do trabalho.

2 CONCEITOS BÁSICOS

Neste capitulo iremos descrever os principais elementos que formam uma RSSF, os principais protocolos padronizados e tecnologias mais relevantes para o uso na composição de tais redes. RSSF são basicamente formadas por *ñnodos sensoresò*e interfaces de comunicação sem fio, este paradigma não é uma novidade e surgiu como alternativa de comunicação e de troca de informação, em lugares onde a instalação de uma infraestrutura convencional de redes (cabeada) é inexistente ou muito difícil. As RSSF possuem como característica a capacidade de se auto-organizarem, cooperando de forma mútua, para proceder a entrega das mensagens até o seu destino, As RSSF permitem uma mobilidade muito maior, a figura 1 mostra um modelo de RSSF.

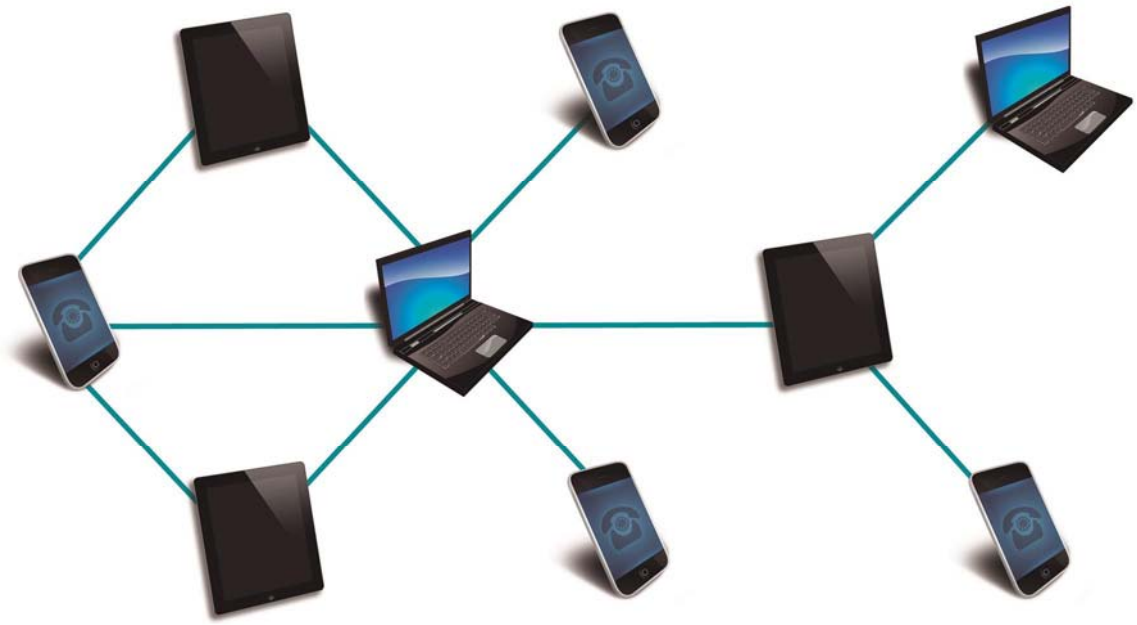

Figura 1 - Modelo de RSSF

Este paradigma não é uma novidade e surgiu como alternativa de comunicação e de troca de informação, em lugares onde a instalação de uma infraestrutura convencional de redes (cabeada) é inexistente ou muito difícil.

(SANTI, 2005) Destaca alguns aspectos que devem ser cuidadosamente observados quando projetamos uma RSSF, são eles:

Conservação de energia: Contrariamente ao caso de redes com fio, RSSF são tipicamente equipadas com fontes de energia limitadas. Assim, usar essa energia restrita de forma eficiente torna-se vital para a manutenção das RSSF. A eficiência energética é especialmente importante em RSSF em que a substituição/recarga de sensores de bateria nem sempre é viável. Utilizando técnicas de conservação de energia em diferentes níveis da arquitetura de uma rede RSSF podemos aumentar, consideravelmente, o tempo de vida das unidades individuais e, consequentemente, da rede propriamente dita.

Largura de banda limitada: Normalmente redes sem fio com múltiplos saltos são caracterizadas por uma largura de banda limitada disponível para os ñósò Embora a largura de banda teórica nas normas industriais tais como IEEE 802.11 pode ser tão elevada como 54MB/seg [IEEE 1999], que a situação tende a piorar na prática, principalmente por interferências causadas por comunicações simultâneas de rádio. Assim, um dos principais problemas no projeto de RSSF é manter a capacidade de suporte do tráfego da rede a um nível razoável.

Variação de tempo e não estruturação da topologia de rede: ñósò da rede podem, em princípio, ser arbitrariamente inseridos e removidos na região de implantação. Assim, o gráfico que representa as ligações de comunicação entre os ñósò é geralmente não estruturado. Além disso, devido à mobilidade e/ou falha de ñóò, a topologia da rede pode variar com o tempo. Dessa forma, se torna difícil determinar o valor apropriado de parâmetros fundamentais de rede.

Comunicações de baixa qualidade: Comunicação sobre canais sem fio é, em geral, muito menos confiável do que nos canais cabeados. Além disso, a qualidade da comunicação é fortemente influenciada por fatores ambientais, que podem ser variáveis no tempo. Considerando que as redes *Ad Hoc* e, especialmente, a RSSF, são suscetíveis de serem implantadas em ambientes hostis. A baixa qualidade de comunicação é um fator presente, em geral, com intervalos não desprezíveis de serviço no tempo.

Operação em ambientes hostis: Em muitos cenários, RSSFs operam em ambientes hostis, de modo que os sensores devem ser explicitamente projetados para trabalhar em condições extremas, que podem acentuar as possibilidades de falhas da unidade individual. Assim, a resiliência às falhas de sensores deve ser explicitamente abordada em diferentes camadas de rede.

Processamento de dados: Dadas as limitações de energia e uma má qualidade de comunicação esperada, sempre que possível, os dados devem ser compactados e/ou agregados com dados de sensores vizinhos, antes de enviá-los para o ñóò(s) gateway.

Escalabilidade: Dependendo do cenário considerado, RSSF pode ser composta por milhares de sensores. Assim, a escalabilidade dos protocolos propostos é uma questão importante.

2.1 TOPOLOGIA E A IMPORTÂNCIA DO SEU CONTROLE

Diferentemente de redes tradicionais, as RSSF não possuem uma topologia fixa e pré-definida, sua característica móvel a torna não estruturada. Sendo assim, as RSSF devem estar preparadas para as mudanças constantes de posições dos ñósò da rede, bem como para as possíveis inclusões e remoções de ñósò Neste sentido, torna-se de suma importância o controle da topologia.

Em redes de sensores sem fio, o uso de controle de topologia se concentra, principalmente, em dois aspectos: prolongamento da vida útil da rede, reduzindo o consumo de energia, e aumentar a capacidade do ñóò de rede (BARONTI, PILLAI, *et al.*, 2007).

Na maioria dos casos os ñósò individuais são alimentados por bateria, por conseguinte, a função dos protocolos de roteamento exerce papel fundamental, a fim de prolongar o tempo de vida da rede, para minimizar o consumo de energia na realização de operações de dados entre os ñósò, sem comprometer a conectividade de rede. Como no caso em que vários caminhos de roteamento estão disponíveis entre a fonte e os ñósò de escoamento, o caminho mais curto pode não ser sempre o mais eficiente, se analisarmos pelo prisma da gerencia de energia. Neste caso o controle de topologia pode ser usado para remover links ineficientes em termos energéticos entre ñósò (BARONTI, PILLAI, *et al.*, 2007).

O segundo aspecto do controle de topologia está relacionada com a capacidade da rede. Na comunicação sem fio, o mesmo meio físico é compartilhado por todos os ñósò, e interferências no canal de comunicação podem ser consideradas transmissões indesejadas de outros ñósò na mesma área. Aumentar a potência de transmissão significa aumentar a gama de interferência com outras comunicações. O Controle da topologia pode ser utilizado, neste caso, para aperfeiçoar a potência do sinal, a fim de reduzir as interferências e, assim, melhorar a capacidade da rede (BARONTI, PILLAI, *et al.*, 2007).

2.2 ROTEAMENTOS EM RSSF

A grande maioria dos protocolos de roteamento existentes é baseada em IP tradicionais, no qual as decisões de encaminhamentos dos pacotes de destino são tomadas com base em tabelas de roteamento que indicam o próximo salto para chegar ao endereço desejado. Em um ambiente RSSF, onde sua atuação geralmente se limita a camada dois, os ñósòpodem ser adicionados aleatoriamente, em quantidades significativas, e a topologia da rede pode variar devido a falhas diversas como, por exemplo, problema no funcionamento dos sensores, falta de energia e sobracarga de mensagens a manutenção da estrutura hierarquica torna-se muito difícil. Sendo assim, os protocolos de roteamento para redes de sensores devem ser leves, tanto para apresentar um processamento adequado, visando os recursos de memórias, quanto exigir o minimo de sobrecarga de menssagens. Preferencialmente, devem ser capazes de rotear pacotes baseados em informações trocadas com seus vizinhos e ser resistente a falhas de ñósò e mudanças na topologia frequentes.

2.2.1 **Roteamento Plano**

No roteamento plano todos os ñósò são considerados iguais do ponto de vista funcional, ou seja, a atividade de roteamento é tratada de forma idêntica por todos os ñósòda rede, como exemplificado na figura 2 (DALTON LUZ, 2004).

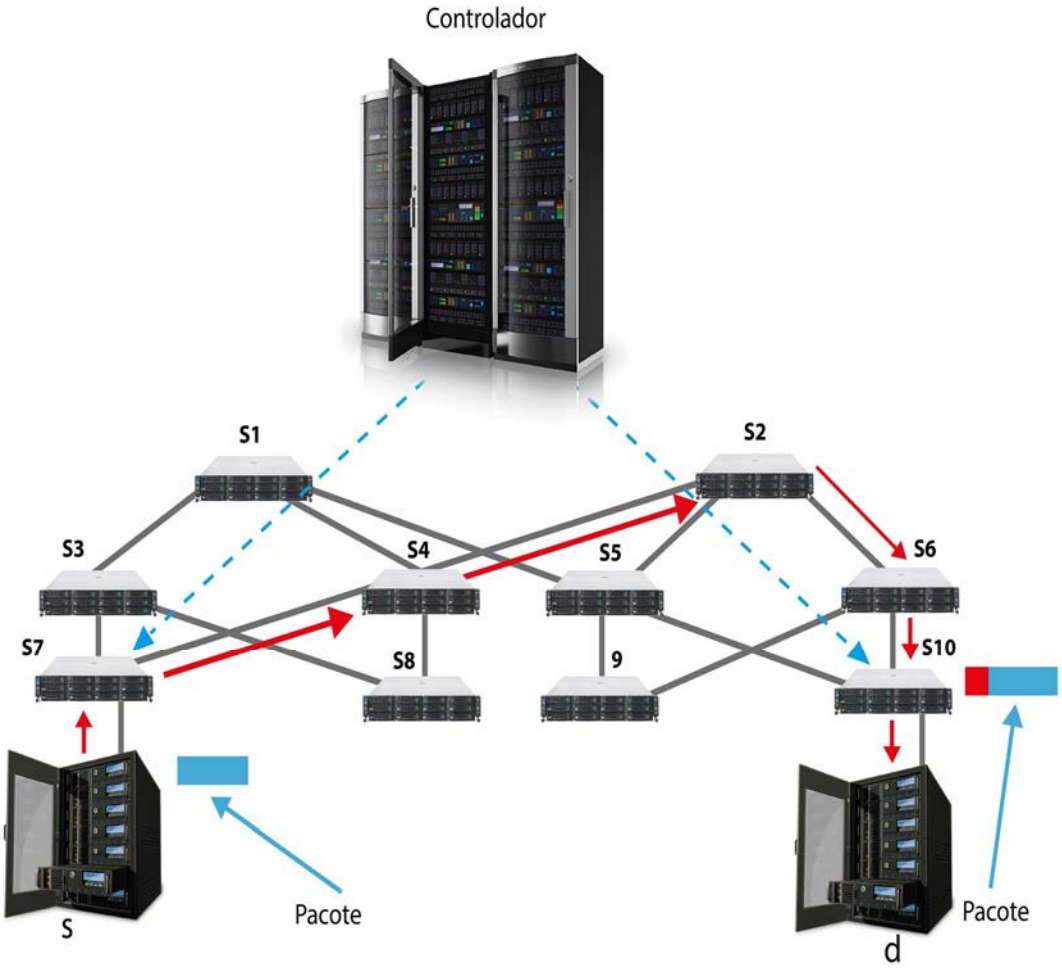

Figura 2 - Roteamento Plano

2.2.2 **Roteamento Hierárquico**

No roteamento hierárquico são estabelecidas duas classes distintas de ñósò ñósò fontes e líderes de grupo (*cluster heads*). Os ñósò fontes simplesmente coletam e enviam os dados para o líder de seu grupo, que pode executar uma fusão/agregação destes dados antes de enviá-lo para o ponto de acesso. Todos os

ñmósò são considerados iguais do ponto de vista funcional, como exemplificado na figura 3 (DALTON LUZ, 2004).

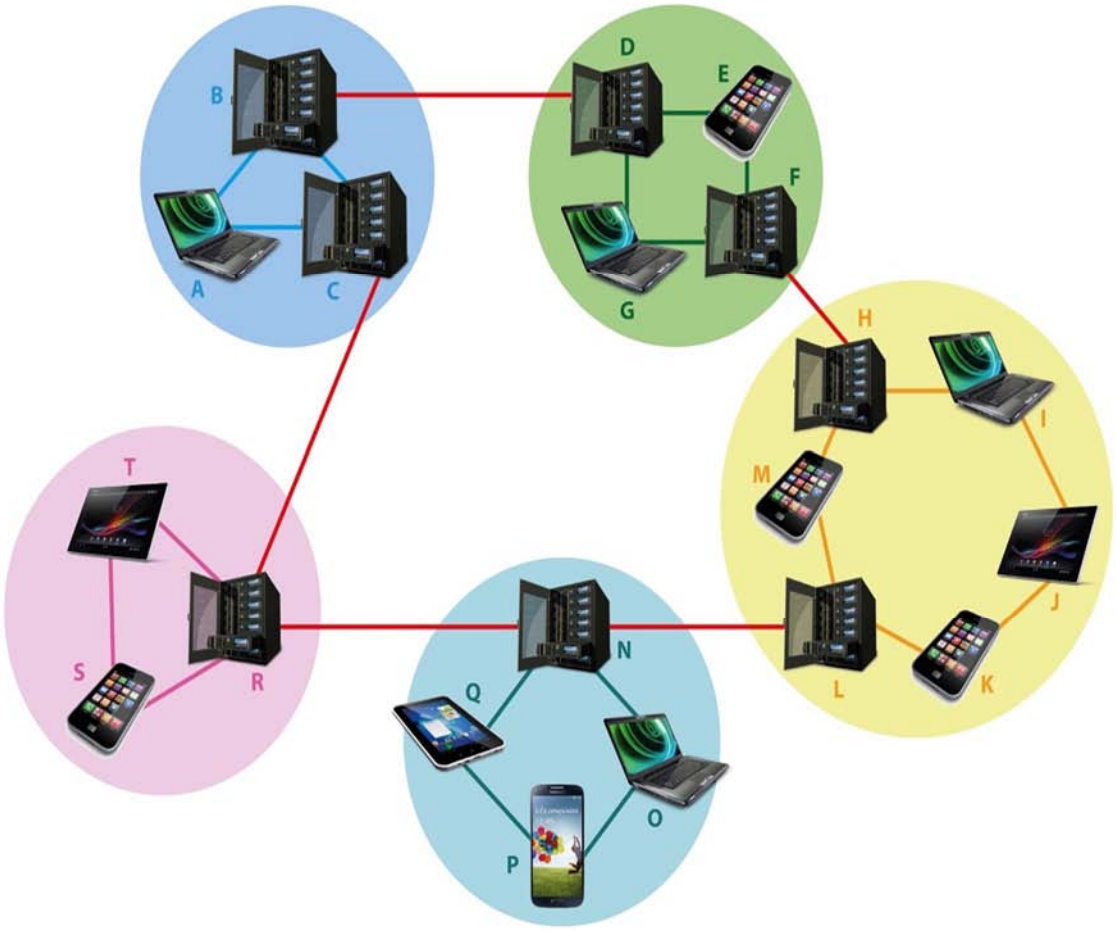

Figura 3 - Roteamento Hierárquico

2.2.3 **Roteamento Geográfico**

O roteamento geográfico utiliza informações geográficas para rotear seus dados. Estas informações costumam incluir a localização dos ñmósò vizinhos. Os dados de localização podem ser definidos a partir de um sistema de coordenadas globais (GPS - *Global Position System*) ou mesmo de um sistema local válido, somente para os ñmósò da rede ou válidos somente para subconjuntos de ñmósò vizinhos, como exemplificados na figura 4 (DALTON LUZ, 2004).

Figura 4 - Roteamento Geográfico

3 ABORDAGEM EM CAMADAS DENTRO IEEE 802.11 SUBESPECIFICAÇÃO RÁDIO E PROTOCOLOS S-MAC E SPIN

Em redes de computadores a conexão entre dispositivos, usualmente, se dá por meio de cabos. Entretanto, apresenta alguns inconvenientes, como limitação de movimento do equipamento, que fica restrito ao tamanho do cabo. Obras estruturais podem ser necessárias para adequar mais dispositivos, a manipulação constante ou incorreta pode fazer com que o conector do cabo se danifique. Felizmente, as redes sem fio estão presentes em nossas vidas e ajudam a dirimir essas restrições. A rede sem fio 802.11 (IEEE, 2007) foi uma das grandes novidades tecnológicas dos últimos anos. Atualmente, é o padrão *de fato* em conectividade sem fio para redes locais. A primeira versão do padrão 802.11 foi lançada em 1997, após sete anos de estudos, aproximadamente. Com o surgimento de novas versões, a versão original passou a ser conhecida como *802.11-1997* ou, ainda, como *802.11 legacy*. Por se tratar de uma tecnologia de transmissão por radiofrequência, o IEEE (*Institute of Electrical and Electronic Engineers*) determinou que o padrão operasse no intervalo de frequências entre 2,4 GHz e 2,4835 GHz. Sua taxa de transmissão de dados era de 1 Mb/s ou 2 Mb/s (megabits por segundo), taxa essa que foi elevada com o surgimento de novas versões, e era possível usar as técnicas de transmissão *Direct Sequence Spread Spectrum* (DSSS) e *Frequency Hopping Spread Spectrum* (FHSS).

A IEEE 1451 é uma família de padrões que define e descreve interfaces para conexão de transdutores (sensores e atuadores), de forma independente de rede de comunicação, a microprocessadores, sistemas de instrumentação e controle, e outros sistemas dotados de transdutores. A característica fundamental dessas

normas é a definição do *Transducer Electronic Data Sheets* (TEDS). O TEDS é uma estrutura de memória que acompanha o transdutor, armazenando dados de identificação, calibração, correção de dados, medição, e de informações relacionadas com a fabricação do transdutor. Uma das metas da1451 é permitir o acesso dos dados dos transdutores através de um conjunto comum de interfaces, estejam os sensores e atuadores ligados a sistemas de redes com ou sem fio (BORTOLASSO TORRI, 2008).

Esta especificação de rádio IEEE 802.11 para o sistema IEEE 1.451,5 fornece uma descrição das funções, protocolos e interfaces que são fornecidos pelo módulo de comunicação IEEE 802.11 entre o módulo de acesso do transdutor, ou WTIM, e o módulo de serviço NCAP. A especificação IEEE 802.11 rádio para IEEE 1451.5, mapas de comandos e mensagens de IEEE 1451,5 da camada superior de convergência, bidirecionalmente através do IEEE 802.11 MAC e PHY para comunicação baseada em rádio entre a WTIM e o Módulo de Serviço NCAP (IEEE, 2007).

A seguir o IEEE 802.11 subespecificação rádio deve ser estruturado de acordo com uma abordagem de rede em camadas, como mostrado na figura 5. IEEE 802.11 devem ser especificados nas camadas um e dois. A escolha de *Internet Protocol* (IP) versão quatro ou versão seis é suportada na camada três. A escolha de *Transmission Control Protocol* (TCP) para ñconectadoò ou *User Datagram Protocol* (UDP) para protocolos de transporte "sem conexão" são suportadas na camada quatro. A "API Shim" é uma fina camada que se encaixa entre o IEEE 1451,0 e IEEE 1451,5 (IEEE, 2007).

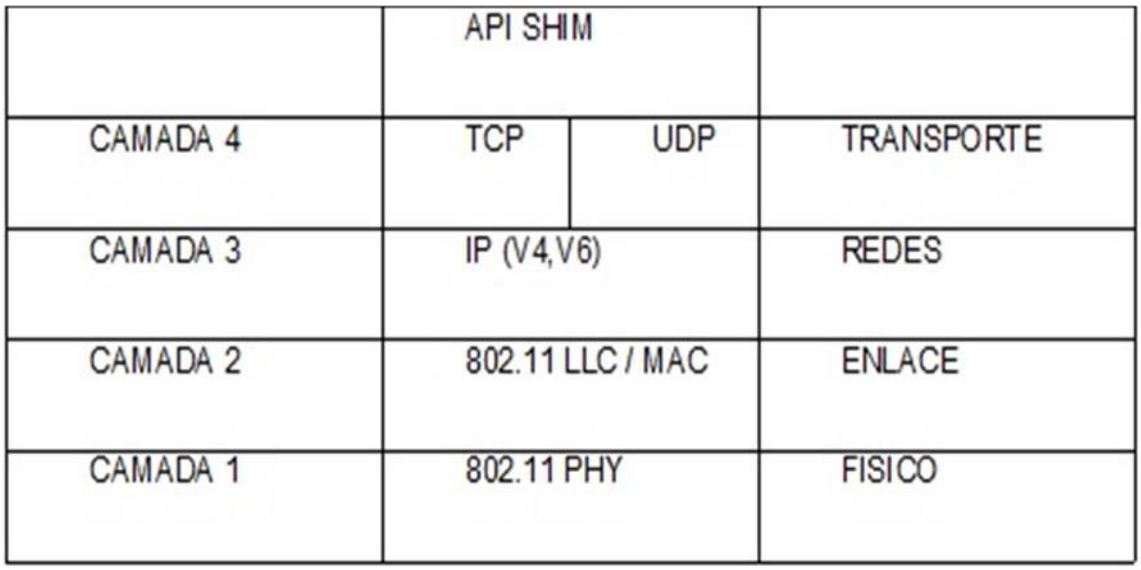

Figura 5 - Especificação de camadas dentro IEEE 802.11 radio subespecificação para o sistema IEEE 1451.5 (IEEE, 2007)

Os detalhes de cada camada devem ser descritos em cláusulas subseqüentes dentro desta especificação funcional. TCP ou UDP na camada 4, e IPv4 ou IPv6 na camada 3, devem ser executados em conformidades com estas especificações funcionais, respectivamente. A pilha de camadas, ilustrado na figura 6, incorpora o "IEEE 802.11 especificação para o sistema de rádio IEEE 1451,5" e logicamente reside em camadas 1- 4 da pilha de rede dentro do módulo de comunicação NCAP e dentro do módulo de comunicação WTIM para um sistema compatível com IEEE 1.451,5 - IEEE 802.11. A fina camada "API Shim" se encaixa entre o IEEE 1451,0 e as IEEE 1451.5 (IEEE, 2007).

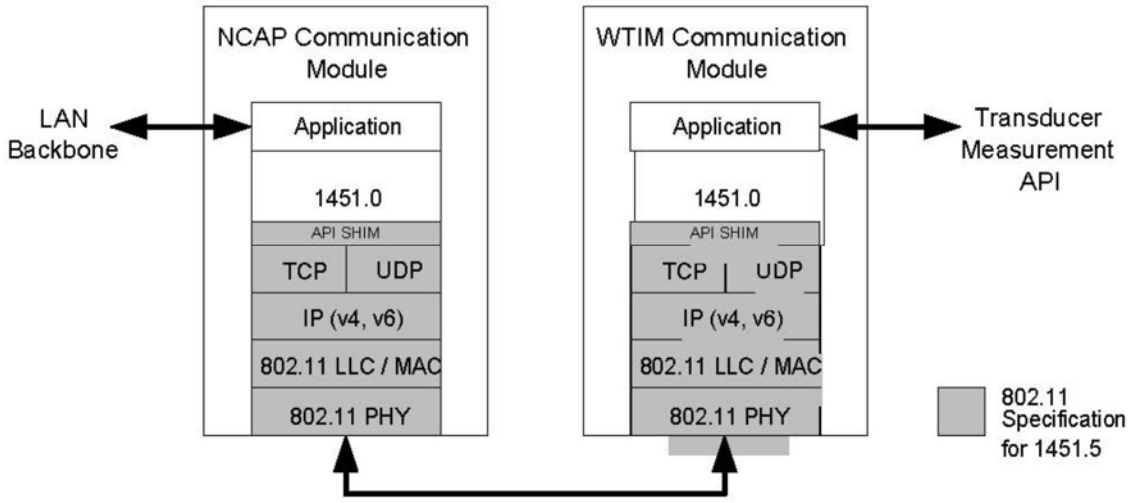

Figura 6 - Estrutura de camadas dentro da NCAP e WTIM (IEEE, 2007)

3.1 MULTIPLOS ESPAÇOS DE ENDEREÇAMENTOS LÓGICOS

Assim como a arquitectura IEEE 802.11 permite uma integração do WM, DSM, a uma LAN com diferentes meios físicos, também permite a possibilidade de que cada um destes componentes possa operar dentro de espaços de endereços diferentes. A arquitetura IEEE 802.11 utiliza e especifica apenas o uso do espaço de endereço WM (IEEE, 2007).

Cada PHY IEEE 802.11 opera em um meio, o WM. O IEEE 802.11 MAC opera em um único espaço de endereço. Os endereços MAC são usados na WM na arquitetura IEEE 802.11. A arquitetura IEEE 802.11optou por utilizar o espaço de endereço IEEE 802 de 48 bits. Assim os endereços IEEE 802.11 são compatíveis com o espaço de endereço utilizado pela família LAN IEEE 802 (IEEE, 2007).

A escolha do espaço de endereçamento no IEEE 802.11 implica em que, para muitas instâncias da arquitectura IEEE 802.11, o espaço de endereço MAC da LAN

cabeada e o espaço MAC de endereço IEEE 802.11 podem ser o mesmo. Nas situações em que um DS usa nível MAC IEEE 802, o endereçamento é apropriado. Todos os três espaços de endereços lógicos usados dentro de um sistema podem ser idênticos. Embora este processo seja comum, não é a única combinação permitida pela arquitectura. A arquitetura IEEE 802.11 permite que todos os três espaços de endereços lógicos possam ser diferentes (IEEE, 2007).

Um exemplo de espaço de endereçamento múltiplo é quando a aplicação DS usa a camada de endereçamento de rede. Neste caso, o espaço de endereço de WM e o espaço de endereço DS seriam diferentes. A capacidade da arquitetura para lidar com mídia e vários espaços de endereço lógico é a chave para a capacidade da arquitetura IEEE 802.11 ser independente da execução DS e servir de interface de rede limpa, com abordagens de mobilidade camada (IEEE, 2007).

3.2 PROTOCOLO DE DESCOBERTA

O objetivo do protocolo de descoberta é a de permitir que ñósò na rede local possam descobrir um ao outro, sem dependência de endereços IP pré-configurados. Também é usado para configurar os endereços de rede. É baseado em um mecanismo de mensagens multicast UDP no endereço 224.0.1.179 e porta 14515. O parâmetro *time-to-live* no cabeçalho IP deve ser padrão para um, de modo que a mensagem de *multicast* atravesse somente a sub-rede local.

Logo após ser ligado, uma vez que uma condição estável for alcançada, cada ñóò IEEE 802.11 1.451,5 transmitirá uma mensagem de "anuncio". E, quando

recebida uma mensagem de "comando", o ñóòtambém deve emitir uma mensagem de "anuncio".

Em um NCAP, a recepção de uma mensagem de "anunciar", a partir de um ponto não reconhecido, deve resultar em uma chamada API, invocando o registerDest (uint8 dotXId, tipo uint8), a camada IEEE 1451,5 802,11 deve interagir diretamente com a API definida entre os sistemas IEEE 1451.0 e IEEE 1451.5, como mostrado na Figura 5. As seguintes informações devem ser armazenadas em cache, localmente, dentro do IEEE 1.451,5 camada de convergência 802.11:".DestID, o endereço IP remoto e porta servidor TCP" Note que o "DestID" é retornado pelo sistema IEEE 1451,0 do 802.11 chamado para IEEE 1451,5 registerDest (uint8 dotXId, tipo uint8).

A carga útil para essas mensagens de *multicast* é codificada em um esquema de ASCII simples, usando um "&" "name = valor" como delimitador. Este formato é modelado após os parâmetros típicos dos mecanismos de codificação da URL (IEEE, 2007).

Três "comandos" de mensagens estão atualmente definidos. O comando *"Discover Request"* é usado para acionar todos os dispositivos para gerar uma mensagem "Responder". O comando "descoberta *Request*" contém os seguintes campos: Versão, command flag indication, o padrão suportado. O comando "Configuração Endereço IP estático" é usado para configurar os parâmetros de endereço de rede. À medida que a mensagem é enviada via multicast, o campo de endereço MAC é proporcionado para especificar o destinatário pretendido. Ele

contém os seguintes campos: Endereço IP, Mascará da subrede, endereço de gateway, endereço MAC, Versão, command flag indication, o padrão suportado (IEEE, 2007).

3.3 COMUNICAÇÃO TCP UNICAST

Logo após a iniciação, uma vez que uma condição estável é atingida, cada ñóò IEEE 802.11- 1451,5 dentro da camada de convergência deve abrir um TCP "ouvir" socket em uma porta arbitrária. No entanto, esta porta é fornecida como parte do protocolo de descoberta já discutido. O ñóò IEEE 802.11 1.451,5 deve se preparar para receber o tráfego de entrada TCP nesse soquete. Durante a fase de registro, cada destino está registrado com o sistema IEEE 1451,0.

Na chamada aberta feita pelo sistema IEEE 1.451,0, este deve passar o "DestID" adequado através da API, para a camada de convergência IEEE 802.11 1.451,5. Essa mesma camada de convergência IEEE 802.11 deve usar "DestID" para procurar o endereço IP, nome de host e porta de destino em seu cache local. Esta informação é usada para abrir um soquete de TCP para o dispositivo remoto. Caso o TCP "Open" seja bem sucedido, um "commId" será criado e armazenado em cache, com o descritor de socket apropriado. Além disso, o IEEE 1451,0 "Open" deve retornar *true.*

Durante a chamada de escrita ou de leitura, o sistema IEEE 1.451,0 deve passar de volta para baixo da *"commId",* logo a camada IEEE 802.11- 1.451,5 deve recuperar o descritor de socket a partir do *cache* local (IEEE, 2007).

3.4 S-MAC E SPIN

Conforme apresentado por (EMERENCIANO, 2005), o fato das RSSF utilizarem baterias e, em grande parte estar localizadas em locais de difícil acesso, a preocupação quanto ao consumo de energia é sempre presente em qualquer projeto de RSSF. Tendo como base o exposto, os protocolos que irão ser utilizados pelas RSSF devem utilizar a energia de uma maneira bem eficiente, elevando assim, o tempo de vida útil do sistema.

Considerando o problema citado, foi apresentado o S-MAC (*Sensor Medium Access Control*). Este protocolo regula o acesso ao meio para as RSSF, e para isso, o S-MAC faz com que os ñósò se tornem ativos, em decorrência do fenômeno desejado (EMERENCIANO, 2005). Para isso, ele utiliza três técnicas:

1. Inatividade de ñósòcom o intuito de reservar energia;
2. Formação de clusters entre ñósò para realizarem auto sincronização; e
3. Transmissão/Recepção sem fio ficam em modo inativo durante transmissões para outros ñósò

As RSSF devem trabalhar com certa tolerância a falha dos sensores, que podem ser ocasionadas por fim da vida útil da bateria ou inoperância dos sensores. Estas falhas não devem ser percebidas por outros ñósò da RSSF e uma maneira de se fazer isto é utilizar a replicação de informação (item 4.1).

Os protocolos SPIN (*Sensor Protocols for Information via Negotiation*) conforme abordado por (EMERENCIANO, 2005), são protocolos adaptativos para

disseminação de dados em RSSF. ñósò que utilizam os protocolos de comunicação SPIN transmitem meta-dados, que é uma espécie de dicionário de dados contendo um conjunto de informações para serem analisadas e a partir da análise, determinar a necessidade de aplicação dos dados em questão, eliminando assim, a redundância de informação na RSSF. Os protocolos SPIN apresentam um ótimo desempenho se levarmos em consideração o desempenho e economia de energia. Existem diversos tipos de protocolos SPIN, tais como:

SPIN-PP/SPIN-EC ï Redes de Sensores sem Fio ponto-a-ponto

SPIN-BC/SPIN-RL ï Redes de Sensores sem Fio broadcast

4 APLICABILIDADE DE REDES SENSORES EM AMBIENTE MILITAR E SEGURANÇA

São muitas as áreas de atuação das redes sensores atualmente. Elas vão de atividades como o monitoramento ambiental, segurança, detecção de velocidade, temperatura e pressão, monitoramento de movimento físico de objetos e uma variedade de aplicações militares (MANJUNATHA, VERMA e SRIVIDYA, 2008).

Neste contexto, uma infinidade de possibilidades surge para a aplicabilidade de redes sensores nas atividades militares, desde detecção de movimentação inimiga, explosões de minas terrestres, localização de meios de combates e presença de material hostil como radiação ou tóxico. Neste capítulo abordaremos as possibilidades de aplicação de redes sensores em ambientes militares, bem como da segurança necessária para o seu adequado funcionamento, e os riscos que este tipo de tecnologia está sujeito, para isto, começaremos falando de um fator primordial para o correto funcionamento desta tecnologia, que é a fusão de dados.

4.1 FUSÃO DE DADOS

Devido à popularização das comunicações de dados, aplicações diversas com um alto grau de acurácia nos dados fornecidos e uma tecnologia em crescente evolução a quantidade de dados fornecidos por uma RSSF é consideravelmente elevada nos dias de hoje.

Comparando ao passado, onde ocorriam transmissões tradicionais, no qual os dados chegavam de diversas formas, sem a preocupação com a redundância dos

mesmos, e os problemas como economia de bateria e processamento não eram tão críticos como em uma RSSF a figura 7 ilustra este tipo de transmissão.

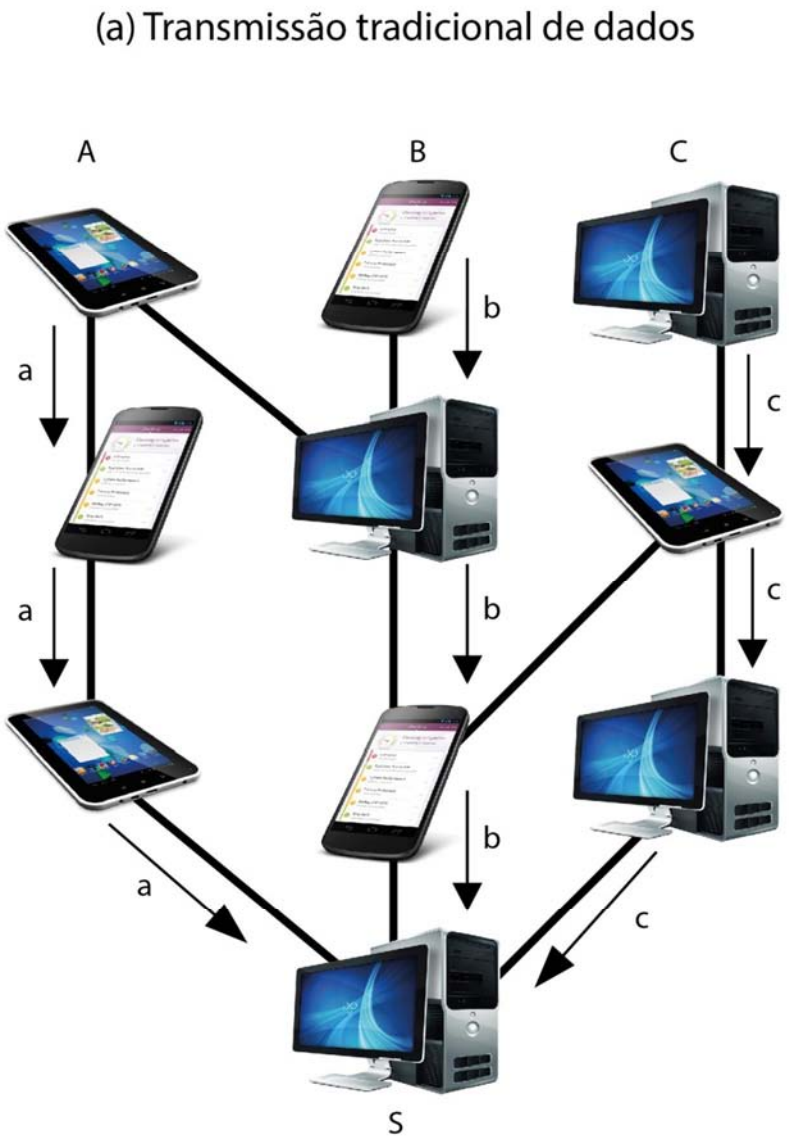

Figura 7 - Transmissão Tradicional de Dados

O grande desafio apresentado em uma RSSF é exatamente filtrar estas informações que muitas vezes podem ser redundantes. Neste cenário, é de suma importância que haja um método para reunir e compilar os dados provenientes dos

diversos sensores de uma RSSF, para que o operador possa ter subsídios na tomada de uma decisão mais adequada. Um problema presente, e que deve ser tratado, no monitoramento feito por RSSF, é a quantidade de dados apresentados pelas RSSF. Neste contexto, a Fusão de Dados figura como uma solução possível para o problema descrito, tratando uma gama de diferentes informações, oriundas de diversos dispositivos, podemos observar um ilustrativo desta transmissão na figura 8.

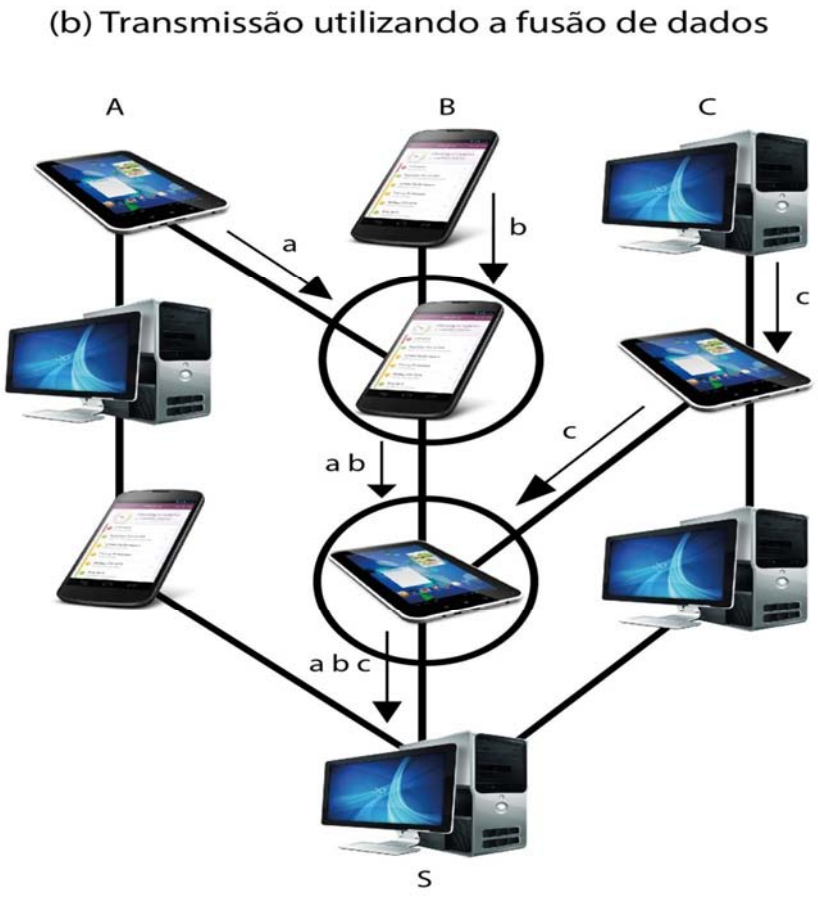

Figura 8 - Transmissão utilizando Fusão de Dados

A maior parte do trabalho de investigação na rede de sensores sem fio é feito no sentido de melhorar e aumentar a vida útil da rede de sensores, propondo novas

formas de energia e protocolos de roteamento eficientes. Grande parte do trabalho também é feito no intuito de agregação de dados, técnica esta usada para aumentar a eficiencia do ñóò sensor e prolongar a duração da bateria, melhorando assim, o tempo de vida de uma rede de sensores.

Esta seção apresenta o novo método de detecção de eventos em RSSF. Considerou-se a detecção de incêndio como um exemplo para detecção de eventos. No sistema de detecção de incêndios tradicionais, vários sensores, como o sensor de monóxido de carbono (CO), o sensor de densidade do fumo e o sensor de temperatura são utilizados para detectar o fogo. Estes sensores de dados são acessados através do fio.

Em arquitetura de *cluster*, os sensores estão agrupando-se para formar um *cluster* com um ñóò central chamado de *cluster head* (CH). O algoritmo de agrupamento particiona a rede em áreas menores chamadas *clusters*. Há um número de algoritmos de clusterização propostos para RSSF em diferentes contextos. A arquitetura de uma RSSF baseada em *cluster* é mostrada na figura 9. Todos os ñósò sensores enviam seus dados para o CH, que agregam e transmitem apenas os dados significativos para o *skin*, ou seja, *Station Base* (BS). O *skin* coleta os dados de todo o CH, que transmite os dados para o usuário via Internet ou via satélite.

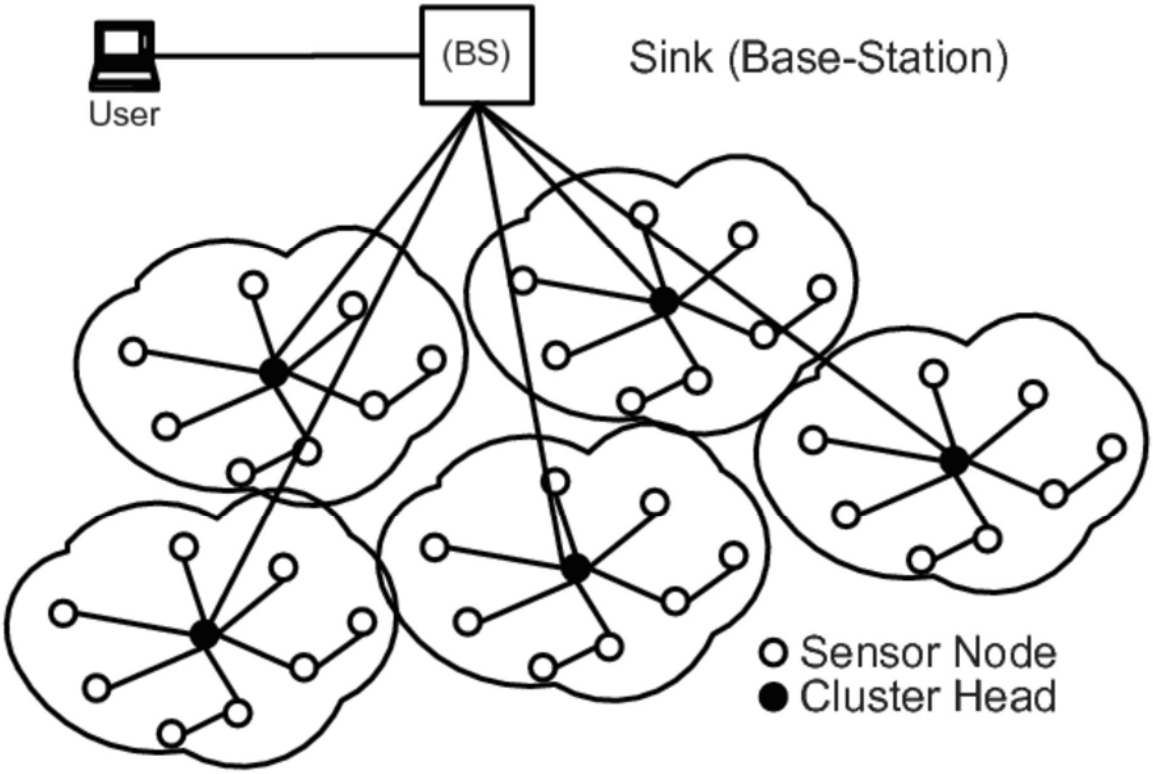

Figura 9 - Arquitetura de Redes Sensores

A lógica *fuzzy* se encaixa melhor em aplicações em que as variáveis são contínuas ou os modelos matemáticos não existem ou modelos de sistemas tradicionais se tornam excessivamente complexa. RSSF é tipicamente utilizado para monitorar alguns parâmetros de um processo no ambiente. Os eventos atmosféricos incorporam em sua natureza, um considerável grau de complexidade, ambíguidade e imprecisão. Por conseguinte, uma abordagem difusa é uma opção viável. O modelo de sistema de lógica *fuzzy*, como mostrado na figura 10, consiste em fuzificação, regras difusas, sistema de inferência *fuzzy* e processo de defuzzificação (MANJUNATHA, VERMA e SRIVIDYA, 2008).

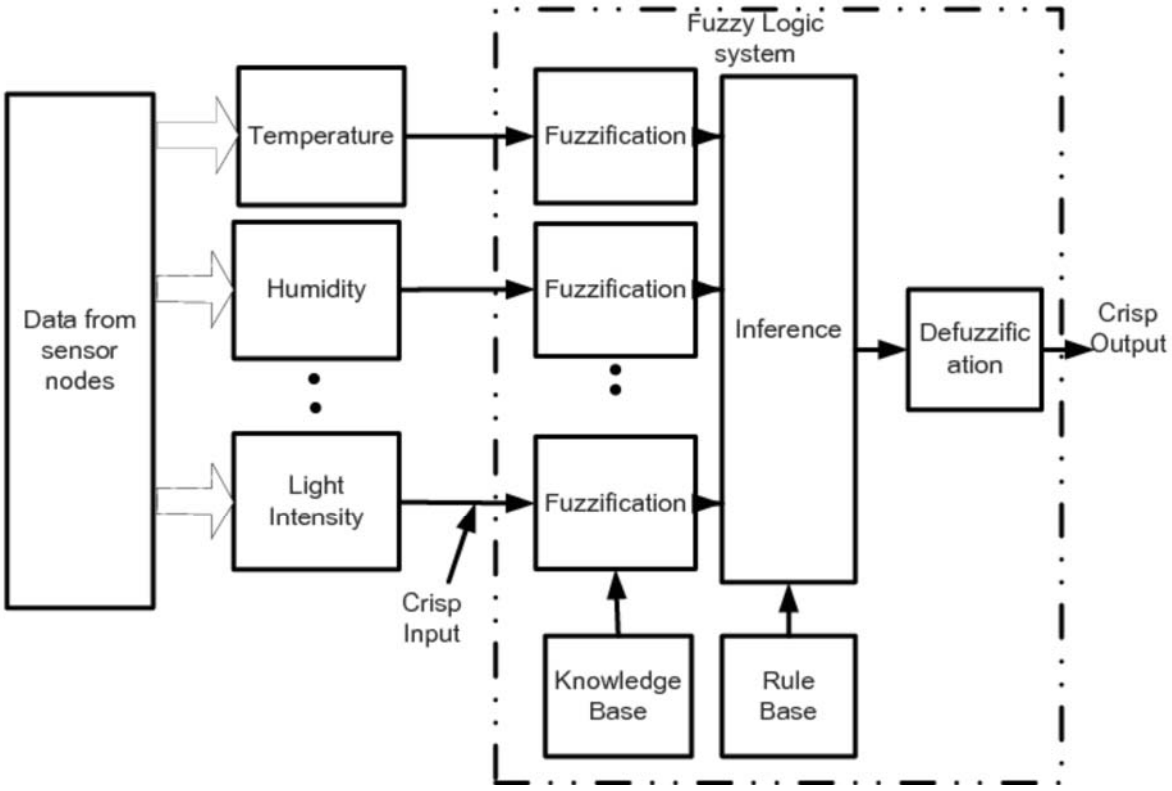

Figura 10 - Estrutura de sistema de lógica fuzzy com múltiplos sensores

4.1.1 **Fuzzification**

Fuzzification é o processo de transformação de valores *crisp* (Um conjunto *crisp* é uma coleção de elementos com algumas propriedades e cada elemento é pertencente ou não a um determinado grupo. Em conjunto *crisp*, não há ambiguidade) em variáveis lingüísticas *fuzzy*.

A função membro é usada para associar um grau a cada variável linguística. A Seleção do número de funções de pertinência e seus valores iniciais se baseiam no conhecimento do processo e intuição. A função de membro tem um valor entre 0 e 1 em um intervalo de variável *crisp*. O número de funções membro pode variar para fornecer a resolução necessária. Número de regras pode crescer

exponencialmente à medida que o número de funções de pertinência de entrada aumenta (MANJUNATHA, VERMA e SRIVIDYA, 2008).

4.1.2 **Sistema de Inferência Fuzzy**

O sistema de inferência *fuzzy* consiste em regras *fuzzy* (*IF* antecedente *ELSE* consequente) que são concebidos por uma base de conhecimento especializado ou por meio de sistema de aprendizagem de insumo-produto. Gaussian, triângulo e trapézio são as funções de pertinência mais comumente usadas. Nas regras difusas, funções triangulares e trapezoidais em forma de adesão são utilizadas para as variáveis, no intuito de simplificar os cálculos. O núcleo do sistema *fuzzy* baseado em regras que imitam o raciocínio humano. A técnica de inferência *fuzzy* mais comumente utilizado é o método de Mamdani. Base de regras *fuzzy* impulsiona o sistema de inferência para produzir saídas difusas, que passam pelo processo de *defuzzification* para obter saídas do sistema (MANJUNATHA, VERMA e SRIVIDYA, 2008).

4.1.3 **Defuzzification**

A transformação de um conjunto *fuzzy* para um número *crisp* é chamada *defuzzification*. Há muitos tipos de métodos de *defuzzification*, normalmente a filiação máxima e técnicas centróide são utilizadas. Na prática, *defuzzification* é feito usando o método centróide (MANJUNATHA, VERMA e SRIVIDYA, 2008).

4.2 RSSF EM AMBIENTES MILITARES

Imaginemos o seguinte cenário: uma zona de conflito de guerra onde um grupo hostil avança em progressão contínua no terreno, com o claro intuito de tomar a sua

posição, seria extremamente valioso se soubessemos quantos soldados esse grupo possui para fazer essa tentativa de assalto à posição, se eles estão se projetando no terreno em marcha ou se estão sendo tripulados por veículos, quais veículos são esses e, que tipo de armamento possui, se portam armas quimicas ou não, quanto tempo demoraria a chegar a um determinado ponto e etc.

Todas essas informações seriam de alta relevância na preparação das tropas, que poderiam se adequar melhor e de forma mais realista para o combate que se apresentaria. Felizmente, nos dias de hoje, as RSSF são amplamente utilizadas, em especial pelo fato de não precisar estabelecer uma infraestrutura clássica de comunicação e transmissão de dados em áreas comprometidas por operações de conflitos.

4.2.1 **Principais Aplicações de RSSF em Ambientes Militares**

A aplicabilidade de RSSF em ambientes militares é bem vasta e complexa, devido ao grau de segurança que deve ser considerado. Neste Contexto, faremos uma breve apresentação das inúmeras aplicabilidades das redes sensores em ambientes militares.

Localização e monitoramento: Ter a possibilidade de saber a posição exata de um soldado e em que parte do terreno a tropa inimiga está localizada, saber se existem minas terrestres ou não, permitindo o avanço seguro da tropa, efetuar o sensoriamento do solo permitindo a detecção de ataques biológicos, nucleares ou químicos, possibilitar que os soldados saibam o posicionamento de tropas inimigas e etc.. Tudo isso é possível com a instalação de sensores nos uniformes dos soldados

e a distribuição de sensores no campo de batalha, isto permite à central monitorar a posição e os movimentos de cada elemento combativo e das tropas inimigas. A utilização deste recurso pode permitir que orientações fossem passadas em tempo real no campo de batalha, possibilitando um aumento considerável no sucesso da missão.

Controle de equipamentos: Poder monitorar o funcionamento de armas e equipamentos, prevendo um possível incidente, controle de munição e monitoramento de combustíveis de veículos. Estes controles são possíveis com a instalação de sensores nos equipamentos e armas utilizadas em campo de batalha.

Sistemas de Mira : Auxiliam os soldados, navios e caças no controle e na precisão de acertos em alvos previamente determinado, principalmente em casos de alvos móveis ou em situações de pouca visibilidade, como ambientes noturnos, nebulosos ou com obstáculos.

Treinamento: Possibilita o adestramento da tropa e preparação de táticas de combates com o uso de jogos de simulação de guerra.

Movimentação: Neste contexto, para ambientes militares, redes *Ad Hoc* fazem mais sentido, pois possuem algumas características próprias que podem ser assim resumidas: uma cadeia de comando bem definida, que pode impactar na topologia da rede; as unidades (grupos de ñósò) que devem cooperar umas com as outras, uma vez que, normalmente, compartilham uma missão; e as operações militares, que tipicamente são conduzidas dentro de limites espaço-temporais bem definidos. Esses fatores implicam em restrições à mobilidade dos ñósò da rede, em

especial no controle da aleatoriedade do movimento (M. PEREIRA e P.PEDROZA, 2004).

4.2.2 **O Modelo JDL**

Devido ao grande escopo dos procedimentos e aplicações possíveis de serem realizadas com os dados, foram propostos alguns modelos de classificação dos sistemas, segundo suas funcionalidades e os níveis de dados com que as aplicações trabalham. Esses modelos, de diferentes laboratórios e grupos de pesquisa, acabaram por ser unificados em um modelo que sofreu colaboração de diversas organizações de pesquisa e é, atualmente, em geral aceito pela literatura da área como padrão de referência de funcionalidade e terminologia para os sistemas de fusão de alvos. O modelo foi criado a partir da fundação, em 1986, do *Joint Directors of Laboratories Data Fusion Working Group*, que originou, logo após, a publicação do modelo, chamado de *Joint Directors of Laboratories Data Fusion Group Model*, ou simplesmente JDL. Após a primeira versão do modelo, houve algumas revisões, que incorporaram novas funcionalidades de maior nível. O JDL é um modelo conceitual que identifica processos e técnicas, e não um modelo de processo, em que os dados fluem de um nível para outro. A abrangência do modelo não se restringe ao campo militar, e tem sido empregado na classificação de sistemas da área de processos, robótica e medicina (DE CARVALHO JÚNIOR, 2010).

O JDL é um modelo conceitual para sistemas de fusão de alvos, que identifica e detalha cada processo necessário a um determinado objetivo de fusão, separando esses processos em níveis de acordo com a quantidade de informação agregada

aos dados com que o sistema daquele nível trabalha. De forma bem genérica, pode-se dizer que foram propostos os seguintes níveis de sistemas:

Nível 0: Pré-processamento de dados de sensores: adaptação do interfaceamento com os sensores (ótico/magnético/elétrico) para leitura dos sinais, conversão de codificação (analógica/digital), translações de espaço (fase/frequência/amplitude), filtragem de ruído e demais tratamentos de sinais necessários à obtenção de dados confiáveis no escopo do sensor tratado.

Nível 1: Processamento de objetos: fusão de dados oriundos de diferentes sensores com o objetivo de determinar a posição, velocidade, aceleração e rumo do alvo.

Nível 2: Análise de contexto: interpretação do contexto composto pelos alvos, o ambiente geográfico, as condições climáticas, o relacionamento dos alvos entre si e com o cenário geográfico de forma a identificar novas entidades como: formaturas de alvos, padrões de movimento e ações de engajamento que estejam em curso.

Nível 3: Análise de impacto: estabelece hipóteses de evolução do cenário tático, procurando prever as consequências da evolução do contexto atual, frente aos alvos presentes, às entidades identificadas e às ações em curso. Procura identificar as ações previsíveis dos entes envolvidos e as ações recomendáveis ao operador do sistema.

Nível 4: Refinamento do processo: monitora a evolução do processo de fusão, procurando correções de alto nível na utilização ou ponderação dos sensores

envolvidos na obtenção das informações dos níveis 1 a 3. Pode determinar o sensor mais adequado para obter informações sobre um determinado alvo, alterar os parâmetros dos algoritmos de fusão de dados multi sensores e detectar falhas de equipamentos.

Nível 5: Refinamento cognitivo ï introduz a avaliação humana *on-line* de especialistas ou operadores do sistema, no sentido de orientar a interpretação do contexto e a produção de conclusões para o processo de tomada de decisão.

Os processos desses diversos níveis lidam com dados que são oriundos de: sensores, informações produzidas por processos de níveis inferiores, informações armazenadas em bancos de dados e de dados de tutoria introduzidos pelos operadores dos sistemas. Além disso, as informações produzidas pelos sistemas são, em alguma instância, apresentadas aos operadores dos sistemas através de uma Interface Homem-Máquina (IHM) (DE CARVALHO JÚNIOR, 2010).

4.3 MECANISMOS DE SEGURANÇA E PROTOCOLOS

(RATHOD e MEHTA, 2011) Abordam dois mecanismos de segurança que são eles mecanismos de baixo nível e de alto nível.

4.3.1 **Mecanismo de segurança de baixo nível**

É primordial para a criação de redes sensores, especialmente em ambientes onde a segurança é vital, o estabelecimento de chaves criptográficas. Geralmente os dispositivos sensores têm limitado poder computacional e as chaves criptográficas

públicas são muito extensas. As Técnicas de estabelecimento de chaves precisam de escalas para redes com centenas ou milhares de ñósò

ñósò sensores podem ter de configurar as chaves com os seus vizinhos e com dados agregados de outros ñósò A desvantagem dessa abordagem é que um atacante com tempo suficiente, empenhado e com muitos ñósò a sua disposição poderia reconstruir o conjunto de chaves completo e quebrar o esquema.

Sigilo e autenticação também são primordiais, as maiorias das aplicações de redes de sensores necessitam de uma proteção contra a espionagem, injeção, e modificação dos pacotes. A criptografia é o padrão defesa comumente utilizado, entretanto, problemas podem ocorrer quando incorporamos a criptografia em redes sensores (criptografia fim a fim por ponto de comunicação), pois aumentamos consideravelmente o nível de segurança, em contra partida as chaves configuradas entre todos os pontos finais devem ser incompatíveis com a participação passiva e difusão local. Como alternativa podemos utilizar criptografia de camada de *enlace* com uma grande rede compartilhando uma chave, o que simplifica a configuração da chave e apoia a participação passiva e difusão local, mas ñósò intermediários podem espionar ou alterar mensagens (RATHOD e MEHTA, 2011).

Como outras redes tradicionais, as redes de sensores devem se preocupar com a robustez e com a privacidade, bem como com a segurança no roteamento de dados. Este é um serviço crucial para permitir a comunicação em redes de sensores. Infelizmente, protocolos de roteamento atuais sofrem em demasiado com problemas de vulnerabilidade de segurança. Por exemplo, um invasor pode lançar ataques de

negação de serviço visando causar um funcionamento anormal em um protocolo de roteamento, impedindo a comunicação. Os ataques mais simples envolvem injetar informações de roteamento malicioso na rede, resultando em inconsistências de roteamento.

Uma das questões mais desafiadoras em redes de sensores é a resiliência contra ataques de captura ñóò Na maioria das aplicações, ñósò sensores são suscetíveis de serem colocados em locais de fácil acesso para os atacantes. Tal exposição levanta a possibilidade de que um invasor pode capturar ñósò sensores, extrair segredos criptográficos, modificar a sua programação, ou substituí-los por ñósò maliciosos sob o controle do atacante. Produzir uma caixa resistente à violação pode ser uma defesa, mas é caro, uma vez que a tecnologia atual não fornece um alto nível de segurança. Por isso, soluções algorítmicas para o problema da captura ñóòsão preferíveis.

4.3.2 **Mecanismo de segurança de alto nível**

Quando abordamos a segurança em alto nível, em redes sensores, começamos a nos preocupar com questões como: a gerência da segurança de grupos onde cada ñóò em uma rede de sensores sem fio possuem, geralmente, limitações na sua capacidade de computação e de comunicação. No entanto, é interessante que a agregação de dados de rede e a análise possa ser realizada por grupos de ñósò Consequentemente, são necessários protocolos de segurança para a gestão de grupo, admitindo de forma segura, membros novos e apoiar a comunicação segura do grupo. O resultado da chave de grupo computacional é

normalmente transmitido para uma estação base. A saída deve ser autenticada para garantir que ela vem de um grupo válido.

Outro fator que merece relevante destaque é a segurança na agregação dos dados, pois os valores detectados devem ser agregados para evitar enormes quantidades de tráfego para a estação de base. Dependendo da arquitetura da rede de sensores sem fio, a agregação pode ocorrer em muitos locais na rede e todos esses locais de agregação devem ser seguros. Detecção de intrusão aplicada para identificar ataques contra a própria rede de sensores é primordial para obtermos uma rede mais segura, em vez de aplicações de detecção de intrusão populares, que são utilizadas em redes convencionais. O que está sendo pesquisado é um sistema de detecção para uso como perímetro de monitoramento, e assim por diante.

4.4 PROTOCOLOS DE SEGURANÇA

Como já foi mencionado, devido à natureza das informações tratadas e o grau de sigilo exigido, na maioria das atividades, a segurança em um ambiente militar é primordial, em especial nas RSSF, onde os requisitos de segurança são difíceis de disponibilizar devido à natureza não estrutura da rede, a conectividade intermitente e a limitação de recursos. Abordaremos alguns protocolos de segurança que se propõem a dirimir os problemas de invasões e acessos não autorizados em RSSF.

4.4.1 **Protocolos de segurança para redes sensores**

O SPINS (*Security Protocols for Sensor Networks*) é composto por dois protocolos. O εTESLA e o SNEP, o εTESLA fica com a função de fornecer

autenticação nas comunicações em broadcast. Já o SNEP é o responsável por prover confidencialidade, autenticação da comunicação ponto a ponto e atualização dos dados sempre tentando obter um *overhead* baixo. O SNEP utiliza num contador que é compartilhado entre transmissor e receptor, esse contador funciona como um vetor de inicialização, para que o algoritmo de criptografia utilizado possa criptografar e decriptografar os dados. Devido à limitação dos sensores, tanto de energia como de processamento, os algoritmos utilizados para criptografia são menos robustos, porém não deixam de ser eficazes. Como ambos participantes possuem o contador, que é incrementado após cada bloco de dados criptografados, o mesmo não precisa ser enviado a cada transmissão (EMERENCIANO, 2005).

Um código de autenticação de mensagem é utilizado com o intuito de obter a autenticação entre transmissor e receptor e, assim, manter a integridade dos dados. Chaves simétricas, emulando assimetria, são utilizadas pelo ***ε****TESLA* com o intuito de evitar que a chave utilizada seja enviada para alguém desautorizado, desta forma, ele consegue autenticar a comunicação em broadcast. Para que isso ocorra é necessário que o protocolo envie, ponto a ponto, para cada ñóò integrante da rede, os parâmetros necessários para a comunicação ser segura. Assinatura digital assegura a autenticidade (EMERENCIANO, 2005).

A assimetria introduzida pelo εTESLA se deve à característica do protocolo que atualiza a chave criptográfica simétrica e somente transmite em broadcast, no final de intervalos de tempo pelas Estações Rádios Base (ERB). De posse dessa chave, os receptores poderão confeccionar cadeias de chaves, autenticando as chaves recebidas, que devem pertencer à cadeia de chaves computadas. Os

Ataques de repetição passam a ser evitados, pois os ñósò identificam o intervalo que a chave recebida pertence e não a utilizam novamente (EMERENCIANO, 2005).

4.4.2 **Protocolo de roteamento tolerante a intrusões para RSSF**

O INSENS parte do pressuposto que um ñóò malicioso só consegue prejudicar os ñósò da vizinhança e nunca a rede como um todo. O INSENS tenta evitar ataques principalmente os de negação de serviço DoS (*Denial of Service*), só a ERB tem permissão para realizar inundações na rede, e para evitar que um ñóò malicioso não se passe pela ERB, a mesma possui uma autenticação junto à RSSF.

Com o intuito de eliminar a possibilidade de introdução de rotas falsas, a ERB dissemina e processa todas as rotas da rede enviando posteriormente as tabelas de rotas autenticadas para os ñósò da rede, evitando assim, que um ñóò malicioso tente inserir uma rota de comunicação falsa na rede. Algoritmos de criptografia simétrica são utilizados com o intuito de atingir a confidencialidade e autenticidade das informações. Dessa forma, são utilizados algoritmos de criptografia simétrica, pois são funcionais e mais leves que os demais tipos de algoritmos de criptografia, dirimindo um sério problema das RSSF, que é a energia, pois por serem mais leves e funcionais acabam gastando menos recursos energéticos. Utilizando o envio de dados por rotas diversas possibilita que, caso seja identificado um ñóò intruso, caminhos alternativos sejam usados, evitando o ñóò intruso (EMERENCIANO, 2005).

4.5 CLASSIFICAÇÃO DA SEGURANÇA

(RATHOD e MEHTA, 2011) Classificam os principais aspectos da segurança das redes sem fios em 3 grandes grupos que são: os obstáculos para a segurança das redes sem fio, os requisitos da RSSF e os ataques. Abordaremos de forma sucinta cada um deles, sempre procurando fazer uma correspondência com as atividades militares.

4.5.1 **Os obstáculos para a segurança das RSSF**

Certamente ao se projetar uma RSSF sabemos que escassez de recursos como energia, memória e espaço de armazenamento é algo que teremos que administrar ao longo da existência da rede, em um ambiente militar este cenário não se altera, soma-se a isso a dificuldade de acesso, onde possivelmente, estas redes estariam instaladas em zonas de guerras, acometidas por desastres naturais e sob ataque inimigo.

Outro fator de suma importância em uma RSSF com finalidade militar é a comunicação e a perda de pacotes na rede, pois troca de mensagens e transferência de pacotes em uma rede insegura pode causar sérios prejuízos à missão. É necessário que haja um mecanismo que trata essa possível perda de pacotes, com o intuito de minimizar os danos causados, este tratamento pode ser dado via *software*.

Os conflitos e a latência também devem ser tratados de forma especial, pois mesmo se o canal é de confiança, a comunicação pode ainda não ser confiável. Isto é, devido à natureza da transmissão de RSSF. Caso os pacotes se encontrem no

meio de transferência, os conflitos ocorrerão e a própria transferência falhará. Em um aglomerado (elevada densidade) de rede de sensores, este pode ser um grande problema. Já o caso da latência ocorre devido ao roteamento com múltiplos saltos, ao congestionamento da rede e ao processamento dos ñnósò, podendo conduzir a uma maior latência na rede, assim dificultando a sincronização entre os ñnósò

Uma das facilidades apresentadas pelas redes sensores é que elas podem executar tarefas, sem que haja uma constante interferência humana, em especial nas atividades militares, onde elas podem estar localizadas em áreas de grande perigo e risco para as tropas.

Neste sentido, algumas precauções devem ser tomadas quanto à exposição dos ñnósò sensores a ataques físicos de tropas inimigas e às condições climáticas, que podem ser bem severas, quanto ao gerenciamento remoto de uma rede de sensores, que se torna praticamente impossível detectar adulteração física e problemas de manutenção.

Um cenário que ilustra muito bem esta situação é um ñnóò sensor utilizado para missões de reconhecimento remoto atrás das linhas inimigas. Em tal caso, o ñnóò não pode ter qualquer contato físico com a tropa amiga, ficando isolado. Ao se projetar uma rede de sensores, principalmente em situações de conflitos, é interessante que ela seja distribuída, pois um ponto de gerenciamento central torna-se alvo de hostilidades inimigas, entretanto ela deve ser concebida corretamente para não ocasionar ineficiência (RATHOD e MEHTA, 2011).

4.5.2 **Requisitos de segurança**

Quando é desenvolvido um projeto de redes, seja ela convencional ou redes sensores, a segurança é fator importantíssimo e que deve ser levado em consideração em qualquer uma das fases de desenvolvimento. Tratando-se de RSSF para ambientes militares, essa preocupação cresce exponencialmente. Neste tópico abordaremos alguns dos principais requisitos de segurança, que devem ser levados em consideração quando se planeja o desenvolvimento de uma RSSF para atividades militares.

Um dos principais focos de uma RSSF é a confidencialidade dos dados. (RATHOD e MEHTA, 2011) Mencionam que uma rede de sensores não deve vazar as leituras dos sensores para os seus vizinhos, especialmente numa aplicação militar, os dados armazenados no ñóò sensor podem ser altamente sensíveis. Em muitas aplicações os dados transmitidos são altamente sensíveis, como por exemplo, a distribuição de chaves. Por conseguinte, é de extrema importância a construção de um canal seguro, em uma rede de sensores sem fio. Informações, tais como identidades de sensores e chaves públicas, também devem ser criptografadas em certa medida, para proteger contra ataques de análise de tráfego.

Com o artifício da confidencialidade, um elemento hostil pode ser incapaz de roubar informações. No entanto, isso não significa que os dados estão seguros. O inimigo pode alterar os dados, de modo a tentar causar desordem a RSSF. Por exemplo, uma tropa inimiga pode adicionar alguns fragmentos ou manipular os dados dentro de um pacote, usando um ñóò malicioso, este novo pacote pode,

então, ser enviado para o receptor original. Assim, a integridade dos dados recebidos assegura que quaisquer dados não foram alterados em trânsito.

O quesito disponibilidade para uma RSSF com aplicações no campo bélico pode significar o sucesso ou fracasso de uma operação, que nesse último caso pode ocasionar baixas na tropa. Algumas abordagens optam por fazer alterações em seus códigos no intuito de reutiliza-lo ao máximo, outras tentam fazer uso de comunicação adicional para alcançar o mesmo objetivo, já outras tentam impor limitações estritas sobre o acesso a dados, às vezes utilizando de um esquema inadequado (como um esquema ponto central), a fim de simplificar o algoritmo. Dessa maneira, todas estas abordagens enfraquecem a disponibilidade de uma RSSF, pelo seguinte motivo: a computação adicional consome mais energia e consequentemente, não havendo mais energia, ocorrerá indisponibilidade dos dados. Comunicação consome mais energia e aumenta a probabilidade da ocorrência de conflitos na RSSF. Caso a abordagem utilizada seja um ponto central, qualquer ação maliciosa neste ñóò poderá ser disseminada para toda a RSSF, ameaçando severamente a disponibilidade da rede.

A maioria das aplicações de redes de sensores depende de alguma forma de sincronização. No intuito de conservar energia, um rádio sensor pode ser desligado por períodos de tempo ou, dependendo da aplicação, quando não houver atividade para monitorar, como, por exemplo, uma RSSF que destinasse a monitoramento da presença inimiga em alguma área específica, que só pode ser acionada quando for detectado algum movimento na área. Além disso, os sensores podem calcular o atraso ñfim a fimòde pacotes. Uma rede de sensores mais colaborativa pode exigir a

sincronização de grupo para aplicações de rastreamento, monitoramento de soldados e etc (RATHOD e MEHTA, 2011).

Uma força inimiga não se limita apenas a modificar o pacote de dados. Ele pode mudar todo o fluxo de pacotes através da injeção de pacotes adicionais e maliciosos. Assim, o receptor precisa assegurar que os dados utilizados em qualquer processo de tomada de decisão procedam de uma fonte correta e confiável, a autenticação dos dados permita que um receptor verifique a procedência dos dados enviados e assim valide este remetente. A autenticação dos dados pode ser alcançada através de um mecanismo de simétrica: o emissor e o receptor compartilham uma chave secreta para computar o código de autenticação de mensagem (MAC) de todos os dados comunicados.

4.5.3 **Ataques**

Redes de sensores são particularmente vulneráveis a vários tipos de ataques e quando se trata de uma RSSF destinada às atividades militares, este cenário não se altera. Os ataques podem ser realizados de várias maneiras, mais notadamente como ataques de negação de serviço, mas também através de análise de tráfego, violação de privacidade, ataques físicos e assim por diante. RSSF são vulneráveis a ataques de segurança devido à natureza da transmissão e do meio de transmissão. (RATHOD e MEHTA, 2011) Abordam os ataques às RSSF sobre dois prismas, um deles são os ataques passivos e o outro são os ataques ativos, seguindo essa linha, abordaremos alguns desses ataques.

Ataques passivos a RSSF militares tem o objetivo de efetuar a vigilância e escuta do canal de comunicação por atacantes não autorizadas. Podemos fazer um exercício e imaginarmos o prejuizo que seria causado se uma operação militar fosse interceptada por tropas inimigas. Certamente o elemento surpresa estaria comprometido e a vantagem que poderia ser obtida não se concretizaria, causando comprometimento da missão.

Na verdade, muita informação a partir de RSSF provavelmente poderia ser recolhida através da vigilância no local. Tudo se agrava porque as RSSF trafegam grandes volumes de informações por meio de acesso remoto. Alguns dos ataques passivos mais comuns contra RSSF são:

Monitoramento: Este é o ataque mais comum à privacidade. Monitorando os dados, a tropa inimiga poderia facilmente descobrir o conteúdo da comunicação. Quando o tráfego transmite informações de controle sobre a configuração de RSSF, conténdo informações potencialmente mais detalhadas do que é acessível através do servidor local, a espionagem pode agir de forma eficaz contra a proteção da privacidade (RATHOD e MEHTA, 2011).

Análise de tráfego: Mesmo quando as mensagens são transferidas criptografadas, elas ainda deixam uma grande possibilidade de análise dos padrões de comunicação. Atividades sensores podem potencialmente revelar informações suficientes para permitir que um inimigo possa causar danos maliciosos à RSSF (RATHOD e MEHTA, 2011).

Camuflagem Inimiga: Pode-se inserir um ñóò ou comprometer um ñósò, já existente na rede, para ficar camuflado na RSSF como um ñóò válido. Depois disso, esse ñóò pode se comportar como um ñóò normal para atrair os pacotes, em seguida, os pacotes podem ser desviados e, conduzindos para uma fonte inimiga, o que já se caracterizaria como um ataque ativo (RATHOD e MEHTA, 2011).

Ataques ativos a RSSF militares ocorrem sobre a camada de rede e tem o objetivo, em sua grande maioria, atingir o roteamento dos pacotes. A seguir será descrito alguns dos possíveis ataques que podem ocorrer neste caso e outros que podem afetar não só a camada de rede.

Spoofed: Um roteamento desprotegido fica vulnerável a esses tipos de ataques, como cada ñóò age como um roteador, qualquer ação maliciosa pode afetar o roteamento da RSSF. Estas ações podem criar loops de roteamento, prolongar ou encurtar as rotas de serviço, gerar mensagens de erro falsas e aumentar o tempo fim-a-fim do pacote (RATHOD e MEHTA, 2011).

Sybil Attack: Em muitos casos, os sensores de uma RSSF poderão trabalhar em conjunto para realizar uma determinada tarefa, portanto, eles podem usar a distribuição de sub-tarefas e redundância de informação. Em tal situação, um ñóò pode pretender ser mais que um ñóò usando as identidades dos outros ñósò legítimos. Este tipo de ataque onde um ñóò forja as identidades de mais de um ñóò é o ataque *Sybil*. Ataque *Sybil* tenta degradar a integridade dos dados, segurança e utilização de recursos que o algoritmo distribuído tenta alcançar. *Sybil* ataque pode ser realizado para atacar o armazenamento distribuído, mecanismo de roteamento,

dados agregados, votação, a alocação de recursos justa e detecção de mau comportamento (RATHOD e MEHTA, 2011).

Black hole/Sinkhole Attack: Neste ataque, um ñóò malicioso age como um buraco negro para atrair todo o tráfego na rede de sensores. Especialmente em um protocolo baseado inundações, o atacante escuta pedidos de rotas, em seguida, responde aos ñósò de destino que ele contém a qualidade ou caminho mais curto para a estação base. Uma vez que o dispositivo malicioso inimigo tenha sido inserido entre os ñósò legítimos ele é capaz de fazer qualquer coisa com os pacotes que passam entre eles (RATHOD e MEHTA, 2011).

Hello Flood Attack: Este ataque usa pacotes *HELLO* como uma arma para convencer os sensores em RSSF. Neste tipo de ataque um inimigo com uma transmissão de radio potente e de longo alcance pacotes *HELLO* a um número de ñósò sensores que estão dispersos em uma grande área dentro de uma RSSF. Os ñósò sensores são, portanto, convencido de que o adversário é seu vizinho. Como consequência, ao enviar as informações para a estação base, os ñósò vítima tentar enviar mensagens através do atacante, que eles entendem ser um vizinho legítimo (RATHOD e MEHTA, 2011).

Denial of service: O mais simples ataque de negação de serviço tenta esgotar os recursos disponíveis para o ñóò vítima, enviando pacotes extras desnecessários e, portanto, impede que os usuários legítimos da RSSF acessem serviços ou recursos aos quais têm direito. Ataque DoS é destinado não só para a tentativa do adversário para subverter, perturbar ou destruir uma rede, mas também

para todo o evento que diminui a capacidade de uma rede para fornecer um serviço. Em RSSF, vários tipos de ataques DoS em diferentes camadas pode ser realizada. Na camada física os ataques DoS poderia ser de adulteração, na camada de enlace, colisão e exaustão, na camada de rede, desorientação dos pacotes e na camada de transporte este ataque poderia ser realizado por inundações maliciososas e ressincronização . Os mecanismos para evitar ataques DoS incluem o investimento em recursos de rede de segurança na rede, autenticação forte e identificação de tráfego (RATHOD e MEHTA, 2011).

Ataques físicos: Redes de sensores normalmente operam em ambientes expostos e hostis, em especial nas atividades militares. Nesses ambientes, os sensores são dispostos sem vigilância o que os torna altamente suscetíveis aos ataques físicos. Ao contrário de muitos outros ataques mencionados anteriormente, ataques físicos tendem a destruir sensores permanentemente, de modo que as perdas são irreversíveis. Por exemplo, os atacantes podem extrair segredos criptográficos, mexer com o circuito associado, modificar a programação dos sensores, ou substituí-los por sensores maliciosos sob o controle do atacante (RATHOD e MEHTA, 2011).

Interrupção de ñmósòMensagens corrompidas: Interrupção de ñmósò é a situação que ocorre quando um ñmóò para de exercer a sua função. Numa interrupção de ñmóò, os protocolos da RSSF devem ser suficientemente robustos para mitigar os efeitos de falhas de ñmóò, proporcionando uma rota alternativa. Bem como, qualquer modificação do conteúdo de uma mensagem por um atacante comprometa a sua integridade (RATHOD e MEHTA, 2011).

Ataques de replicação de ñóò Conceitualmente, um ataque de replicação ñóò é bastante simples: um atacante tenta adicionar um ñóò a uma RSSF existente copiando o ID de um ñóò sensor válido existente. Um ñóò replicado nesta abordagem pode perturbar gravemente o desempenho de uma rede de sensores. Os pacotes podem ser corrompidos ou mesmo desviados de sua rota original. Isso pode resultar no desconectamento da rede, falsas leituras dos sensores e etc. Caso um atacante ganhe o acesso físico de toda a rede, ele pode copiar chaves criptográficas para os ñósò sensores replicadas. Ao inserir os ñósò replicados em pontos específicos da rede, o invasor pode facilmente manipular um segmento específico da rede, talvez por desconectá-lo completamente (RATHOD e MEHTA, 2011).

5 **CONCLUSÃO**

Neste trabalho descrevemos os principais elementos que formam uma RSSF, os principais protocolos padronizados e as tecnologias mais relevantes para o uso na composição de tais redes. Expusemos os problemas apresentados por uma RSSF como, por exemplo, a necessidade de se gerir de forma consciente, energia, capacidade de processamento e largura de banda, pois todos estes recursos são extremamente limitados. Apresentamos a importância do uso do controle de topologia, principalmente nos aspectos de prolongamento da vida útil da rede, reduzindo o consumo de energia, aumentando assim, a capacidade do ñóòde rede. Abordamos de forma sucinta os roteamentos planos, hierárquicos, geográficos e o padrão 802.11, que é responsável por tornar viável a existência de uma rede sem fio.

Podemos observar que as possibilidades de aplicação de redes sensores em ambientes Militares são enormes, desde a segurança de áreas e instalações, passando por ações em campos de batalhas e ajudando no treinamento e adestramento de tropas. Entretanto, evidenciou-se a importância de considerar seriamente os níveis de segurança, pois é necessário que os dados trafegados e as informações obtidas sejam manipulados com critérios, evitando o vazamento e garantindo o sigilo. Neste contexto os protocolos de segurança bem como os mecanismos de criptografia exercem papel fundamental para tentar garantir a integridade dos dados.

Tendo em vista o exposto, surge como forte tendência o desenvolvimento de Redes Sensores que consigam gerir seus recursos, hoje extremamente escassos,

de forma mais inteligente com o objetivo de prolongar a sua vida útil. No que tange a área militar, fazer uso de RSSF para criar situações de adestramento o mais próximo da realidade possível preparando de uma forma mais eficaz o elemento de combate para as situações reais. Executar planejamentos precisos na área de logística dimensionando dias de operações, alimentação necessária, carga e tipo de equipamentos adequado para a situação, tudo isso tomando por base as informações atualizadas de dimensões de terreno, tipo de missão e dificuldades apresentadas.

Outra linha de ação no futuro é o desenvolvimento de protocolos que se mostrem mais eficientes com a questão do monitoramento e comunicação entre os ñósò, em constante movimento e apresentando distâncias maiores entre eles. Ser capaz de mapear constantemente a posição dos ñósò em campo de combate, mesmo em distâncias maiores, impõe um grande desafio a ser vencido, haja vista que a referida evolução deve estar em consonância com requisitos robustos de segurança, a fim de garantir os requisitos básicos da Segurança da Informação Digital e o não comprometimento de dados sigilosos.

6 **BIBLIOGRAFIA**

BARONTI, P. et al. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. **Computers communication**, 2007. 1655-1695.

BORTOLASSO TORRI, L. A norma IEEE 1451 aplicada a redes heterogêneas de sensores sem fio. **Universidade Federal de Santa Catarina**, Floriaòpólis, Santa Catarina, outubro 2008. 14-83.

DALTON LUZ, G. Roteamento em Redes Sensores. **Instituto de Matemática e Estatística Universidade de São Paulo**, São Paulo, novembro 2004. 4-35.

DE CARVALHO JÚNIOR,. Fusão de Dados Multi-Nível em Ambientes de Monitoração Continuo de Sistemas Táticos Navais Utilizando Múltiplas Lógicas. **COPPE, da Universidade Federal do Rio de Janeiro**, Rio de Janeiro, março 2010.

DUTRA, R. C. Redes Ad Hoc Centradas em Interesses para Ambientes Móveis. **Universidade Federal do Rio de Janeiro/COOPE**, Rio de Janeiro, março 2012.

EMERENCIANO, J. N. Segurança em Redes de Sensores sem Fio Protocolos e Estratégias de Ataque. **Universidade Presidente Antônio Carlos**, Minas Gerais, 2005.

GOMES, , R. L. et al. Maximização da vida útil de redes de sensores sem fio utilizando fusão de dados e roteamento fuzzy. **XV Workshop de Gerência e Operação de Redes e Serviços/XXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**, Gramado, Rio grande do Sul, 2010.

IEEE. Standard for a Smart Transducer Interface for Sensors and Actuatorsð Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats. **IEEE**, outubro 2007.

LOUREIRO, A. A. F. Redes de Sensores Sem Fio. **Anais do XXII Congresso da SBC**, Floriaòpólis, Santa Catarina, julho 2012.

M. PEREIRA, I. C.; P.PEDROZA, A. D. C. Análise de Redes Móveis Ad Hoc para Cenários de Operações Militares. **Universidade Federal do Rio de Janeiro**, Rio de Janeiro, 2004.

MACHADO, L.; MONTEIRO, D. Gateway Mesh-RSSF: Sistema de Comunicação entre Redes de Sensores Sem Fio e Redes Mesh. **Faculdade de Computação ï Universidade Federal do Pará (UFPA)**, Pará, Belém.

MANJUNATHA, ; VERMA, ; SRIVIDYA,. Multi-Sensor Data Fusion in Cluster based Wireless Sensor Networks Using Fuzzy Logic Method. **Interdisciplinary Program in Reliability Engineering Indian Institute of Technology Bombay**, Mumbai, India, dezembro 2008.

MARGI, C. B. et al. Segurança em Redes de Sensores sem Fio. **IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**, 2009. 149-194.

PERRIG, A. et al. SPINS: Security Protocols for Sensor Networks. **Department of Electrical Engineering and Computer Sciences University of California**, Berkeley, California, 2011.

RATHOD, ; MEHTA,. Security in wireless Sensor Network: A Survey. **Ganpat University Journal of Eengineering & Technology**, Nadiad, Gujarat, India, 1, janeiro-junho 2011. 35-44.

SANTI, P. Topology Control in Wireless Ad Hoc and Sensor Network. **Istituto di Informática e Telematica**, 37, n. 2, junho 2005. 164-194.

SANTOS, A. S. Análise Comparativa de Protocolos Para redes Sensores sem Fio. **Instituto de Matemática e Estatística da Universidade de São Paulo**, São Paulo, outubro 2009. 08-40.

SANTOS, M. A. S. Análise Comparativa de Protocolos de Segurança Para Redes Sem Fio. **USP**, São Paulo, Outubro 2009.

SIMPLÍCIO JÚNIOR, M. A. Algoritmo de Autenticação de Mensagens para Redes Sensores. **USP**, São Paulo, Março 2010.

SONG, E. Y.; LEE,. Understanding ieee 1451-networked smart transducerinterface standard-what is a smart transducer? **Instrumentation & Measurement Magazine, IEEE**, 2008. 11-17.

TIERNO, A. P. Protocolos de Roteamento para RSSFs. **Universidade Federal de Santa Maria**, Santa Maria, Rio Grande do Sul, julho 2008.

YICK, J.; MUKHERJEE, B.; GHOSAL, D. Wireless sensor network survey, 2008.